ICS 35.040
L 80

中华人民共和国国家标准

GB/T 18018—2019
代替 GB/T 18018—2007

信息安全技术
路由器安全技术要求

Information security technology—
Technical requirement for router security

2019-08-30 发布　　2020-03-01 实施

国家市场监督管理总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准代替 GB/T 18018—2007《信息安全技术　路由器安全技术要求》。

本标准与 GB/T 18018—2007 相比，除编辑性修改外主要技术变化如下：

——修改了第 2 章规范性引用文件(见第 2 章，2007 年版的第 2 章)；

——修改了 3.2 缩略语(见 3.2，2007 年版的 3.2)；

——修改了 4.1.2.1 管理员鉴别(见 4.1.2.1，2007 年版的 4.1.2.1)；

——增加了 4.1.3.2 管理协议设置、4.1.4 设备安全防护、4.1.5 安全功能保护；

——修改了 5.1.2.1 管理员鉴别、5.1.3.1 权限管理(见 5.1.2.1、5.1.3.1，2007 年版的 5.1.2.1、5.1.3.1)；

——增加了 5.1.3.2 管理协议设置、5.1.4 设备安全防护、5.1.5 网络安全防护、5.1.6 安全功能保护；

——修改了 6.1.2.1 管理员鉴别、6.1.4.1 权限管理(见 6.1.2.1、6.1.4.1，2007 年版的 6.1.2.1、6.1.4.1)；

——增加了 6.1.2.2 设备登录口令管理、6.1.2.3 证书验证、6.1.3.2 数据存储、6.1.3.3 数据传输、6.1.3.4 敏感数据、6.1.4.2 管理协议设置、6.1.5 设备安全防护、6.1.6 网络安全防护、6.1.7 安全功能保护；

——删除了 5.1.8 路由认证、6.1.10 路由认证；分别调整到 5.1.5.2 和 6.1.6.2 中；

——删除了第 7 章附加安全功能。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位：中国科学院软件研究所、华为技术有限公司、新华三技术有限公司、迈普通信技术股份有限公司、中国科学院信息工程研究所、北京大学软件与微电子学院、中国电子技术标准化研究院。

本标准主要起草人：卿斯汉、陈驰、付天福、王博、杨银柱、李晶林、何斌、王利明、赵志宇、王惠莅、罗锋盈、周启明、沈晴霓、文伟平、马书南。

本标准所代替标准的历次版本发布情况为：

——GB/T 18018—1999、GB/T 18018—2007。

信息安全技术
路由器安全技术要求

1 范围

本标准分等级规定了路由器的安全功能要求和安全保障要求。

本标准适用于路由器产品安全性的设计和实现，对路由器产品进行的测试、评估和管理也可参照使用。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB 17859—1999 计算机信息系统安全保护等级划分准则

GB/T 18336.1～18336.3—2015 信息技术 安全技术 信息技术安全性评估准则

3 术语和定义、缩略语

3.1 术语和定义

GB 17859—1999 和 GB/T 18336.1～18336.3—2015 界定的以及下列术语和定义适用于本文件。

3.1.1

路由器 router

主要的网络节点设备，承载数据流量，通过路由选择算法决定流经数据的转发处理，并可以通过集成防火墙等功能模块提供访问控制和安全扩展功能。

3.1.2

简单网络管理协议 simple network management protocol

一系列协议组和规范，提供了一种从网络上的设备收集网络管理信息的方法，也为设备向网络管理工作站报告问题和错误提供了一种方法。

3.1.3

单播逆向路径转发 unicast reverse path forwarding

为防止基于源地址欺骗的网络攻击，以源地址为目的地址，在转发表中查找源地址对应接口是否与入接口匹配的动作。

3.2 缩略语

下列缩略语适用于本文件。

HTTPS 安全套接字层超文本传输协议(Hyper Text Transfer Protocol over Secure Socket Layer)

IKE Internet 密钥交换协议(Internet Key Exchange Protocol)

IPSec Internet 协议安全(Internet Protocol Security)

LDAP 轻量级目录访问协议(Lightweight Directory Access Protocol)

MPLS	多协议标记交换(Multi-Protocol Label Switching)
RADIUS	远程用户拨号认证系统(Remote Authentication Dial In User Service)
SFTP	安全文件传输协议(Secure File Transfer Protocol)
SNMP	简单网络管理协议(Simple Network Management Protocol)
SNMPV3	简单网络管理协议版本 3(Simple Network Management Protocol Version 3)
SSH	安全壳协议(Secure Shell)
SSL/TLS	安全套接字层/传输层安全协议(Secure Socket Layer/Transport Layer Security)
TACACS	终端访问控制器访问控制系统(Terminal Access Controller Access Control System)
URPF	单播逆向路径转发(Unicast Reverse Path Forwarding)
VPN	虚拟专用网(Virtual Private Network)
VRRP	虚拟路由冗余协议(Virtual Router Redundancy Protocol)

4 第一级安全技术要求

4.1 安全功能要求

4.1.1 自主访问控制

路由器应执行自主访问控制策略,通过管理员属性表,控制不同管理员对路由器的配置数据和其他数据的查看、修改,以及对路由器上程序的执行,阻止非授权人员进行上述活动。

4.1.2 身份鉴别

4.1.2.1 管理员鉴别

在管理员进入系统会话之前,路由器应鉴别管理员的身份,鉴别时应采用口令机制,并在每次登录系统时进行。口令应是不可见的,并在存储和传输时加密保护。

当进行鉴别时,路由器应仅将最少的反馈(如:打入的字符数,鉴别的成功或失败)提供给被鉴别人员。同时,反馈信息应避免提示“用户名错误”“口令错误”等信息,避免攻击者进行用户名或口令的暴力猜解。

4.1.2.2 鉴别失败处理

在经过一定次数的鉴别失败以后,路由器应锁定该账号。最多失败次数仅由授权管理员设定。

4.1.3 安全管理

4.1.3.1 权限管理

路由器应能够设置多个角色,具备划分管理员级别和规定相关权限(如:监视、维护配置等)的能力,能够限定每个管理员的管理范围和权限,防止非授权登录和非授权操作。

4.1.3.2 管理协议设置

路由器应能配置和使用安全的协议对系统进行管理控制。应使用 SSH、SFTP、SNMPV3 和 HTTPS。

4.1.3.3 安全属性管理

路由器应为管理员提供对安全功能进行控制管理的功能,这些管理包括:

a) 与对应的路由器自主访问控制、鉴别和安全保障技术相关的功能的管理。
b) 与一般的安装和配置有关的功能的管理。
c) 路由器的安全配置参数要有初始值。路由器安装后，安全功能应能及时提醒管理员修改配置，并能周期性地提醒管理员维护配置。

4.1.4 设备安全防护

4.1.4.1 流量控制

路由器应能够对设备本身需进行解析处理的协议流量大小进行控制，例如，通过设置带宽等防护手段，保证系统在经受协议泛洪攻击时原有转发业务正常，在泛洪攻击消除后系统可直接恢复。

4.1.4.2 优先级调度

无。

4.1.4.3 资源耗尽防护

无。

4.1.5 安全功能保护

4.1.5.1 自检

设备在上电启动时应执行安全功能的自检，如内存、数字签名、加密算法等，确保安全功能正确。只有当所有自检功能通过时，才能正常启动设备。

4.1.5.2 保证软件更新的合法性

安全管理员应能查询当前执行的软件/固件版本号及最近一次安装的版本号。应能在安装更新前用数字签名验证软件/固件更新的合法性。

4.2 安全保障要求

4.2.1 配置管理

开发者应设计和实现路由器配置管理，为产品的不同版本提供唯一的标识，且产品的每个版本应使用其唯一的标识作为标签。

4.2.2 交付和运行

开发者应以文档形式对路由器安全交付以及安装和启动过程进行说明。文档中应包括：
a) 对安全地将路由器交付给用户的说明；
b) 对安全地安装和启动路由器的说明。

4.2.3 开发

开发者应提供路由器功能设计，要求按非形式化功能设计的要求进行功能设计，以非形式化方法描述安全功能及其外部接口，并描述使用外部安全功能接口的目的和方法。

4.2.4 指导性文档

开发者应编制路由器的指导性文档，要求如下：

a) 文档中应提供关于路由器的安全功能与接口、路由器的管理和配置、路由器的启动和操作、安全属性、警告信息的描述；
b) 文档中不应包含任何一旦泄露将会危及系统安全的信息，文档可以为硬拷贝、电子文档或联机文档。如果是联机文档，应控制对文档的访问。

4.2.5 生命周期支持

开发者应建立开发和维护路由器的生命周期模型，包括用于开发和维护路由器的程序、工具和技术。开发者应按其定义的生命周期模型进行开发和维护，并提供生命周期定义文档，在文档中描述用于开发和维护路由器安全功能的生命周期模型。

4.2.6 测试

开发者应对路由器进行测试，要求如下：
a) 应进行一般功能测试，保证路由器能够满足所有安全功能的要求；
b) 保留并提供测试文档，详细描述测试计划、测试过程以及预测结果和实际测试结果。

5 第二级安全技术要求

5.1 安全功能要求

5.1.1 自主访问控制

路由器应执行自主访问控制策略，通过管理员属性表，控制不同管理员对路由器的配置数据和其他数据的查看、修改，以及对路由器上程序的执行，阻止非授权人员进行上述活动。

5.1.2 身份鉴别

5.1.2.1 管理员鉴别

在管理员进入系统会话之前，路由器应鉴别管理员的身份，鉴别时应采用口令机制，并在每次登录系统时进行。口令应是不可见的，并在存储和传输时加密保护。

当进行鉴别时，路由器应仅将最少的反馈（如：打入的字符数，鉴别的成功或失败）提供给被鉴别人员。同时，反馈信息应避免提示“用户名错误”“口令错误”等信息，避免攻击者进行用户名或口令的暴力猜解。

5.1.2.2 鉴别失败处理

在经过一定次数的鉴别失败以后，路由器应锁定该账号。最多失败次数仅由授权管理员设定。

5.1.2.3 超时锁定

路由器应具有登录超时锁定功能。在设定的时间段内没有任何操作的情况下终止会话，需要再次进行身份鉴别才能够重新操作。最大超时时间仅由授权管理员设定。

注：本标准中的黑体字表示该等级中新出现的增强要求。

5.1.2.4 会话锁定

路由器应为管理员提供锁定自己的交互会话的功能，锁定后需要再次进行身份鉴别才能够重新管理路由器。

5.1.2.5 登录历史

路由器应具有登录历史功能，为登录人员提供系统登录活动的有关信息，使登录人员识别入侵的企图。成功通过鉴别并登录系统后，路由器应显示如下数据：

a) 日期、时间、来源和上次成功登录系统的情况；

b) 上次成功登录系统以来身份鉴别失败的情况；

c) 口令距失效日期的天数。

5.1.3 安全管理

5.1.3.1 权限管理

路由器应能够设置多个角色，具备划分管理员级别和规定相关权限（如：监视、维护配置等）的能力，能够限定每个管理员的管理范围和权限，防止非授权登录和非授权操作。

系统应能支持 RADIUS/TACACS 的集中认证授权管理。

5.1.3.2 管理协议设置

路由器应能配置和使用安全的协议对系统进行管理控制。应使用 SSH、SFTP、SNMPV3 和 HTTPS。

5.1.3.3 安全属性管理

路由器应为管理员提供对安全功能进行控制管理的功能，这些管理包括：

a) 与对应的路由器自主访问控制、鉴别和安全保障技术相关的功能的管理。

b) 与一般的安装和配置有关的功能的管理。

c) 路由器的安全配置参数要有初始值。路由器安装后，安全功能应能及时提醒管理员修改配置，并能周期性地提醒管理员维护配置。

5.1.4 设备安全防护

5.1.4.1 流量控制

路由器应能够对设备本身需进行解析处理的协议流量大小进行控制，例如，通过设置带宽等防护手段，保证系统在经受协议泛洪攻击时原有转发业务正常，在泛洪攻击消除后系统可直接恢复。

5.1.4.2 优先级调度

路由器应能够按照业务重要性对设备本身需进行解析处理的协议流量进行优先级调度。对高优先的协议流量进行优先保证，当发生业务量激增或网络攻击时使重要业务不中断。

5.1.4.3 资源耗尽防护

路由器应能够对重要系统资源进行保护，通过限定资源分配的方式将攻击影响限定到一定范围内。

路由器应支持 MAC 地址学习限制功能，使系统其他接口用户不受影响。

5.1.5 网络安全防护

5.1.5.1 单播逆向路径转发功能

路由器应具备 URPF 功能，在网络边界阻断源 IP 地址欺骗攻击。

5.1.5.2 路由协议认证

路由器使用的路由协议应支持路由认证功能，保证路由是由合法的路由器发出的，并且在转发过程中没有被改变。

5.1.5.3 MPLS VPN 功能

路由器应基于 MPLS 协议实现二层和三层 VPN 功能，采用独立的 VPN 管理网络，实现不同用户间的业务隔离。

5.1.6 安全功能保护

5.1.6.1 自检

设备在上电启动时应执行安全功能的自检，如：内存、数字签名、加密算法等，确保安全功能正确。只有当所有自检功能通过时，才能正常启动设备。

5.1.6.2 安全的软件更新

安全管理员应能查询当前执行的软件/固件版本号及最近一次安装的版本号。应能在安装更新前用数字签名验证软件/固件更新的合法性。

5.1.7 审计

5.1.7.1 审计数据生成

路由器应具有审计功能，至少能够审计以下行为：

a) 审计功能的启动和终止；
b) 账户管理；
c) 登录事件；
d) 系统事件；
e) 配置文件的修改。

路由器应为可审计行为生成审计记录，并在每一个审计记录中至少记录以下信息：

a) 事件发生的日期和时间；
b) 事件的类型；
c) 管理员身份；
d) 事件的结果(成功或失败)。

5.1.7.2 审计数据查阅

路由器应为授权管理员提供从审计记录中读取审计信息的能力，为管理员提供的审计记录具有唯一、明确的定义和方便阅读的格式。

5.1.7.3 审计数据保护

路由器应能保护已存储的审计记录，避免未经授权的删除，并能监测和防止对审计记录的修改。当审计存储耗尽、失败或受到攻击时，路由器应确保最近的审计记录在一定的时间内不会被破坏。

5.1.8 可靠性

路由器应提供可靠性保证，具有部分冗余设计性能。支持插卡、接口、电源等部件的冗余与热插拔

能力。

5.2 安全保障要求

5.2.1 配置管理

开发者应设计和实现路由器配置管理，要求如下：

a) 开发者应使用配置管理系统，**并提供配置管理文档**，为产品的不同版本提供唯一的标识，且产品的每个版本应使用其唯一的标识作为标签。

b) 配置管理范围至少应包括路由器的产品实现表示、设计文档、测试文档、用户文档、配置管理，从而确保它们的修改是在一个正确授权的可控方式下进行的。配置管理文档至少应能跟踪上述内容，并描述配置管理系统如何跟踪这些配置项。

5.2.2 交付和运行

开发者应以文档形式对路由器安全交付以及安装和启动过程进行说明。文档中应包括：

a) 对安全地将路由器交付给用户的说明；

b) 对安全地安装和启动路由器的说明。

5.2.3 开发

开发者应提供路由器功能规范，要求如下：

a) 按非形式化功能设计的要求进行功能设计，以非形式化方法描述安全功能及其外部接口，并描述使用外部安全功能接口的目的和方法。

b) 提供路由器安全功能的高层设计。高层设计应按子系统描述安全功能及其结构，并标识安全功能子系统的所有接口。高层设计还应标识实现安全功能所要求的基础性的硬件、固件和软件。

c) 开发者应提供路由器安全功能的功能设计与高层设计之间的非形式化对应性分析，该分析应证明功能设计表示的所有相关安全功能都在高层设计中得到正确且完备的细化。

5.2.4 指导性文档

开发者应编制路由器的指导性文档，要求如下：

a) 文档中应提供关于路由器的安全功能与接口、路由器的管理和配置、路由器的启动与操作、安全属性、警告信息、**审计工具**的描述。

b) 文档中不应包含任何一旦泄漏将会危及系统安全的信息，文档可以为硬拷贝、电子文档或联机文档。如果是联机文档，应控制对文档的访问。

5.2.5 生命周期支持

开发者应建立开发和维护路由器的生命周期模型，即用于开发和维护路由器的程序、工具和技术。要求如下：

a) 开发者应按其定义的生命周期模型进行开发和维护，并提供生命周期定义文档，在文档中描述用于开发和维护路由器安全功能的生命周期模型。

b) 该模型对于路由器开发和维护应提供必要的控制，采用物理上、程序上、人员上以及其他方面的安全措施保护路由器开发环境的安全，包括场地的物理安全和对开发人员的选择，并采取适当的防护措施来消除或降低路由器开发所面临的安全威胁。

5.2.6 测试

开发者应对路由器进行测试，要求如下：

a） 应进行一般功能测试，保证路由器能够满足所有安全功能的要求。

b） 应提供测试深度的分析。在深度分析中，应论证测试文档中所标识的对安全功能的测试足以表明该安全功能的运行与高层设计是一致的。

c） 应进行相符性独立测试，由专业的第三方独立实验室实施测试，确认路由器能够满足所有安全功能的要求。

d） 保留并提供测试文档，详细描述测试计划、测试过程以及预测结果和实际测试结果。

5.2.7 脆弱性评定

脆弱性评定包含下述内容：

a） 开发者应提供指导性文档和分析文档，在文档中确定对路由器的所有可能的操作方式（包括失败和操作失误后的操作）的后果以及对于保持安全操作的意义，并列出所有目标环境的假设和所有的外部安全措施（包括外部程序的、物理的或人员控制）要求。所述内容应是完备、清晰、一致和合理的。

b） 开发者应对具有安全功能强度生命的安全机制（例如，口令机制）进行安全功能强度分析。安全功能强度分析应证明安全机制达到了所声明的强度。

c） 开发者应实施脆弱性分析，并提供脆弱性分布的文档。对所有已标识的脆弱性，文档应说明它们在所期望的路由器使用环境中不能被利用。文档还应说明如何确保用户能够得到最新的安全补丁。

d） 脆弱性分析文档中应包含对所使用协议的脆弱性分析。

6 第三级安全技术要求

6.1 安全功能要求

6.1.1 自主访问控制

路由器应执行自主访问控制策略，通过管理员属性表，控制不同管理员对路由器的配置数据和其他数据的查看、修改，以及对路由器上程序的执行，阻止非授权人员进行上述活动。

6.1.2 身份鉴别

6.1.2.1 管理员鉴别

在管理员进入系统会话之前，路由器应鉴别管理员的身份。鉴别应支持数字证书等鉴别方法，并在每次登录系统时进行。口令应是不可见的，并在存储和传输时加密保护。

当进行鉴别时，路由器应仅将最少的反馈（如：打入的字符数，鉴别的成功或失败）提供给被鉴别人员。同时，反馈信息应避免提示“用户名错误”“口令错误”等信息，避免攻击者进行用户名或口令的暴力猜解。

6.1.2.2 设备登录口令管理

设备应能够提供身份鉴别管理策略，限制口令的最小长度、组成、复杂度、使用期等。口令组成应支持数字、大小写字母和特殊符号；并能限制历史密码的使用。

设备登录口令不能以明文形式显示或存储，应采用单向函数方式存储，并保证单向函数的强度。

6.1.2.3 证书验证

设备应支持使用证书进行身份验证。例如，SSH、IKE、SSL/TLS 等协议应支持证书认证，增强设备的安全性。颁发证书的 CA 应提供网络设备可访问的 LDAP 或其他证书黑名单访问机制，以确保失效证书访问拒绝。

6.1.2.4 鉴别失败处理

在经过一定次数的鉴别失败以后，路由器应锁定该账号。最多失败次数仅由授权管理员设定。

6.1.2.5 超时锁定

路由器应具有登录超时锁定功能。在设定的时间段内没有任何操作的情况下终止会话，需要再次进行身份鉴别才能够重新操作。最大超时时间仅由授权管理员设定。

6.1.2.6 会话锁定

路由器应为管理员提供锁定自己的交互会话的功能，锁定后需要再次进行身份鉴别才能够重新管理路由器。

6.1.2.7 登录历史

路由器应具有登录历史功能，为登录人员提供系统登录活动的有关信息。成功通过鉴别并登录系统后，路由器应显示如下数据：

a) 日期、时间、来源和上次成功登录系统的情况；
b) 上次成功登录系统以来身份鉴别失败的情况；
c) 口令距失效日期的天数；
d) 证书距过期日期的天数。

6.1.3 数据保护

6.1.3.1 概述

路由器应具有数据完整性功能，对系统中的数据采取有效措施，防止其遭受非授权人员的修改、破坏和删除。

6.1.3.2 数据存储

只有管理员才能管理（包括但不限于：创建、初始化、查看、添加、修改、删除等操作）设备的配置、身份和审计数据。

6.1.3.3 数据传输

管理员应能选择安全协议（例如，SSH、IPSec、TLS 等）对传输的数据进行保护。保护功能包括：身份认证、机密性和完整性。

6.1.3.4 敏感数据

对于敏感数据，例如，用户口令、私钥、对称密钥、预共享密钥等，应以密文的形式显示或存储。

6.1.4 安全管理

6.1.4.1 权限管理

路由器应能够设置多个角色，具备划分管理员级别和规定相关权限（如：监视、维护配置等）的能力，

能够限定每个管理员的管理范围和权限，防止非授权登录和非授权操作。

系统应能支持 RADIUS/TACACS 的集中认证授权管理。

6.1.4.2 管理协议设置

路由器应能配置和使用安全的协议对系统进行管理控制。应使用 SSH、SFTP、SNMPV3 和 HTTPS。

6.1.4.3 安全属性管理

路由器应为管理员提供对安全功能进行控制管理的功能，这些管理包括：

a) 与对应的路由器自主访问控制、鉴别和安全保障技术相关的功能的管理。

b) 与一般的安装和配置有关的功能的管理。

c) 路由器的安全配置参数要有初始值。路由器安装后，安全功能应能及时提醒管理员修改配置，并能周期性地提醒管理员维护配置。

6.1.5 设备安全防护

6.1.5.1 流量控制

路由器应能够对设备本身需进行解析处理的协议流量大小进行控制，例如，通过设置带宽等防护手段，保证系统在经受协议泛洪攻击时原有转发业务正常，在泛洪攻击消除后系统可直接恢复。

6.1.5.2 优先级调度

路由器应能够按照业务重要性对设备本身需进行解析处理的协议流量进行优先级调度。对高优先的协议流量进行优先保证，当发生业务量激增或网络攻击时使重要业务不中断。

6.1.5.3 资源耗尽防护

路由器应能够对重要系统资源进行保护，通过限定资源分配的方式将攻击影响限定到一定范围内。攻击结束后应能释放攻击时路由器分配的资源。

路由器应支持 MAC 地址学习限制功能，使系统其他接口用户不受影响。

6.1.6 网络安全防护

6.1.6.1 单播逆向路径转发功能

路由器应具备 URPF 功能，在网络边界阻断源 IP 地址欺骗攻击。

6.1.6.2 路由协议认证

路由器使用的路由协议应支持路由认证功能，保证路由是由合法的路由器发出的，并且在转发过程中没有被改变。

6.1.6.3 MPLS VPN 功能

路由器应基于 MPLS 协议实现二层和三层 VPN 功能，采用独立的 VPN 管理网络，实现不同用户间的业务隔离。

6.1.7 安全功能保护

6.1.7.1 自检

设备在上电启动时应执行安全功能的自检，如内存、数字签名、加密算法等，确保安全功能正确。只

有当所有自检功能通过时，才能正常启动设备。

6.1.7.2 保证软件更新的合法性

安全管理员应能查询当前执行的软件/固件版本号及最近一次安装的版本号。应能在安装更新前用数字签名验证软件/固件更新的合法性。

6.1.8 审计

6.1.8.1 审计数据生成

路由器应具有审计功能，至少能够审计以下行为：

a) 审计功能的启动和终止；
b) 账户管理；
c) 登录事件；
d) 系统事件；
e) 配置文件的修改。

路由器应为可审计行为生成审计记录，并在每一个审计记录中至少记录以下信息：

a) 事件发生的日期和时间；
b) 事件的类型；
c) 管理员身份；
d) 事件的结果（成功或失败）。

6.1.8.2 审计数据查阅

路由器应为授权管理员提供从审计记录中读取审计信息的能力，为管理员提供的审计记录具有唯一、明确的定义和方便阅读的格式。

6.1.8.3 审计数据保护

路由器应能保护已存储的审计记录，避免未经授权的删除，并能监测和防止对审计记录的修改。当审计存储耗尽、失败或受到攻击时，路由器应确保最近的审计记录在一定的时间内不会被破坏。

6.1.8.4 潜在侵害分析

路由器应能监控可审计行为，并指出潜在的侵害。

路由器应在检测到可能有安全侵害发生时作出响应，如：通知管理员，向管理员提供一组遏制侵害的或采取矫正的行动。

6.1.9 可靠性

框式路由器应具有全冗余设计，应确保无中断在线升级，支持插卡、接口、电源等部件的冗余与热插拔等功能，能够安装双引擎和双电源模块，具有故障定位与隔离及远程重启等功能。盒式路由器至少应提供无中断在线升级的方式，如可使用补丁包方式无中断升级。

路由器可以通过虚拟路由冗余协议 VRRP 组成路由器机群。

6.2 安全保障要求

6.2.1 配置管理

开发者应设计和实现路由器配置管理，要求如下：

a) 开发者应使用配置管理系统，并提供配置管理文档，为产品的不同版本提供唯一的标识，且产品的每个版本应当使用其唯一的标识作为标签。

b) 配置管理范围至少应包括路由器的产品实现表示、设计文档、测试文档、用户文档、配置管理，从而确保它们的修改是在一个正确授权的可控方式下进行的。配置管理文档至少应能跟踪上述内容，并描述配置管理系统如何跟踪这些配置项。

c) 部分的配置管理应实现自动化。

6.2.2 交付和运行

开发者应以文档形式对路由器安全交付以及安装和启动的过程进行说明。文档中应包括：

a) 对安全地将路由器交付给用户的说明。

b) 对安全地安装和启动路由器的说明。

c) 对如何检测路由器在分发过程中发生的未授权修改、如何检测攻击者伪装成开发者向用户交付路由器产品的说明。

以安全方式分发并交付产品后，仍应提供对路由器的长期维护和评估的支持，包括产品中的漏洞和现场问题的解决。

以安全方式分发并交付产品后，仍应不断向用户提供可能会影响到路由器安全的注意事项或警告信息。

6.2.3 开发

开发者应提供路由器功能规范，要求如下：

a) 按非形式化功能设计的要求进行功能设计，以非形式化方法描述安全功能及其外部接口，并描述使用外部安全功能接口的目的和方法。

b) 提供路由器安全功能的高层设计。高层设计应按子系统描述安全功能及其结构，并标识安全功能子系统的所有接口。高层设计还应标识实现安全功能所要求的基础性的硬件、固件和软件。**高层设计还应描述安全功能子系统所有接口及使用接口的目的和方法，并详细描述接口的返回结果、例外情况和错误信息等，以及如何将路由器中有助于增强安全策略的子系统分离出来。**

c) 开发者应提供路由器安全功能的低层设计。低层设计应以模块术语描述安全功能，并描述每一个模块的目的、接口和相互间的关系。低层设计还应描述如何将路由器中有助于增强安全策略的模块分离出来。

d) 开发者应提供路由器安全功能的功能设计与高层设计之间的非形式化对应性分析，该分析应证明功能设计表示的所有相关安全功能都在高层设计中得到正确且完备的细化。

e) 开发者应提供安全策略模型，并阐明该模型和路由器功能设计之间的对应性，这一对应性是一致和完备的。安全策略模型是非形式化的。该模型应描述所有可以模型化的安全策略的规则和特征，并阐明该模型对于所有可模型化的安全策略来说，是与其一致且完备的。

6.2.4 指导性文档

开发者应编制路由器的指导性文档，要求如下：

a) 文档中应提供关于路由器的安全功能与接口、路由器的管理和配置、路由器的启动与操作、安全属性、警告信息、审计工具的描述。

b) 文档中不应包含任何一旦泄露将会危及系统安全的信息，文档可以为硬拷贝、电子文档或联机文档。如果是联机文档，应控制对文档的访问。

6.2.5 生命周期支持

开发者应建立开发和维护路由器的生命周期模型，即用于开发和维护路由器的程序、工具和技术。要求如下：

a) 开发者应按其定义的生命周期模型进行开发和维护，并提供生命周期定义文档，在文档中描述用于开发和维护路由器安全功能的生命周期模型。

b) 该模型对于路由器开发和维护应提供必要的控制，采用物理上、程序上、人员上以及其他方面的安全措施保护路由器开发环境的安全，包括场地的物理安全和对开发人员的选择，并采取适当的防护措施来消除或降低路由器开发所面临的安全威胁。

c) 开发者应描述用于开发路由器的工具和参照标准，并提供关于已选择的开发工具选项的描述文档。开发工具文档应明确说明所有开发工具选项的含义。

6.2.6 测试

开发者应对路由器进行测试，要求如下：

a) 应进行一般功能测试，保证路由器能够满足所有安全功能的要求。

b) 应提供测试深度的分析。在深度分析中，应论证测试文档中所标识的对安全功能的测试足以表明该安全功能的运行与高层设计以及低层设计是一致的。

c) 应进行相符性独立测试，由专业第三方独立实验室或消费者组织实施测试，确认路由器能够满足所有安全功能的要求。

d) 应由专业第三方独立实验室或消费者组织抽样独立性测试。开发者应提供能有效重现开发者测试的必需资料，包括可由机器阅读的测试文档、测试程序等。

e) 保留并提供测试文档，详细描述测试计划、测试过程以及预测结果和实际测试结果。

6.2.7 脆弱性评定

开发者应提供指导性文档和分析文档，在文档中确定对路由器的所有可能的操作方式（包括失败和操作失误后的操作）的后果以及对于保持安全操作的意义，并列出所有目标环境的假设和所有的外部安全措施（包括外部程序的、物理的或人员控制）要求。所述内容应是完备、清晰、一致和合理的。

开发者应对具有安全功能强度生命的安全机制（例如，口令机制）进行安全功能强度分析。安全功能强度分析应证明安全机制达到了所声明的强度。

开发者应实施脆弱性分析，并提供脆弱性分布的文档。对所有已标识的脆弱性，文档应说明它们在所期望的路由器使用环境中不能被利用。文档还应说明如何确保用户能够得到最新的安全补丁。

脆弱性分析文档中应包含对所使用协议的脆弱性分析。

安全功能要求对照表和安全保障要求对照表参见附录 A。

附 录 A
（资料性附录）
安全要求对照表

表 A.1 和表 A.2 分别给出了条款中安全功能要求和安全保障要求的对照表。其中，＋表示具有相应的安全功能要求/安全保障要求；＋＋表示具有比＋增强的要求；＋＋＋表示具有比＋＋增强的要求。

表 A.1 安全功能要求对照表

安全功能要求		第一级	第二级	第三级
自主访问控制		＋	＋	＋
身份鉴别	设备登录口令管理			＋
	证书验证			＋
	管理员鉴别	＋	＋	＋＋
	鉴别失败处理	＋	＋	＋
	超时锁定		＋	＋
	会话锁定		＋	＋
	登录历史		＋	＋＋
数据保护	数据存储			＋
	数据传输			＋
	敏感数据			＋
安全管理	权限管理	＋	＋＋	＋＋
	管理协议设置	＋	＋	＋
	安全属性管理	＋	＋	＋
设备安全防护	流量控制	＋	＋	＋
	优先级调度		＋	＋
	资源耗尽防护		＋	＋
网络安全防护	单播逆向路径转发功能		＋	＋
	路由协议认证		＋	＋
	MPLS VPN 功能		＋	＋
安全功能保护	自检	＋	＋	＋
	保证软件更新的合法性	＋	＋	＋
审计	审计数据生成		＋	＋
	审计数据查阅		＋	＋
	审计数据保护		＋	＋
	潜在侵害分析			＋
可靠性			＋	＋＋

表 A.2　安全保障要求对照表

安全保障要求	第一级	第二级	第三级
配置管理	+	++	+++
交付和运行	+	+	++
开发	+	++	+++
指导性文档	+	++	++
生命周期支持	+	++	+++
测试	+	++	+++
脆弱性评定		+	+